UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,832	08/03/2001	Jack Hong	4366-49	8603

48500 7590 02/09/2006

SHERIDAN ROSS P.C.
1560 BROADWAY, SUITE 1200
DENVER, CO 80202

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 02/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/921,832	HONG, JACK	
	Examiner	Art Unit	
	Kyung H. Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *38-72 and 74-76* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *38-72 and 74-76* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/4, 8/22/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application RCE filed 10/27/2005.

2. Claims **1 - 37** have been canceled. Claims **38, 39, 53, 54, 63, 67, 69, 70** have been amended. Claims **38 - 76** are pending. Claim **73** is missing. Independent claims are **38, 53, 69**.

Response to Arguments

3. Applicant's arguments with respect to claims 38-76 have been considered but are moot in view of the new ground(s) of rejection.

3.1 Applicant argues that the referenced prior art does not disclose *" ... distinguish transaction requests from different clients having a common address on the communications network ... " (see Remarks Page 17, Lines 5-6)*

The Harkinson (6,799,202) prior art discloses the capability for multiple host names for one IP address. (see Harkinson col. 11, lines 46-49: single (i.e. common) IP address for multiple host names (i.e. network entities))

3.2 Applicant argues that the referenced prior art does not disclose *" ... a tag generated by an informational server that identifies uniquely the generating informational server among the various servers in the server farm let alone positioning such a tag in the packet payload ... " (see Remarks Page 17, Lines 7-9)* ; *" ... use of a packet payload tag identifying a target information*

server for use in routing the packet ... " (see Remarks Page 18, Lines 19-20)

The Harkinson (6,799,202) prior art discloses the usage tag information utilized in the selection of an informational server to process a request. (see Harkinson col. 11, lines 59-67: tag mode, packet payload (i.e. message information), message information utilized for server selection, two consecutive messages processed by same switch)

3.3 Applicant argues that the referenced prior art does not disclose *" ... at least one ... " (see Remarks Page 21, Line 10)* Claims disclose *" ... at least one of an invariant, cookie, and a tag ... ".*

The Harkinson (6,799,202) prior art discloses a invariant, cookie, and a tag. (see Harkinson col. 11, lines 64-67: invariant (i.e. previous information remembered) ; col. 18, lines 40-43; col. 21, lines 49-51: cookie ; col. 11, lines 59-67: tag mode, message information utilized for server selection, two consecutive messages processed by same switch)

Claim Rejection - 35 USC § 103

4. **Claims 38, 39, 47 - 51, 53, 54, 61 - 66, 68 - 70, 75, 76** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Harkinson et al.** (US Patent No. 6,799,202) in view of **Williams** (US Patent No. 6,304,973).

Regarding Claim 38, Harkinson discloses an arrangement for serving information requests, comprising:

a) a plurality of informational servers connected to a communications network, all of the informational servers having a common address on the communications network (see Harkinson col. 2, lines 26-28: multiple members (i.e. information servers)) and serving a set of information to clients, each of the informational servers being configured to receive a transaction request associated with an individual transaction and to provide a response to each transaction request; (see Harkinson col. 2, lines 46-54: client information requests, server responses) and

b) a content director (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch, (i.e. content director, information controller)) connecting the informational servers to the communications network and distributing transaction requests among the informational servers comprising:

i) a flow switch that parses plain text transaction requests to locate selected packet payload fields, selects, based on plain text packet payload fields, an appropriate informational server to service each transaction request, and thereafter forwards at least portions of the parsed transaction requests to a selected one of the informational servers; (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch ; col. 11, lines 53-56; col. 11, lines 59-64: identification information utilized for information processing ; col. 2, lines 46-

54: requests processed and passed to servers ; col. 11, lines 59-67: tag mode, message information utilized for server selection) and

Harkinson discloses parsing and informational server selection by the flow switch (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48; col. 11, lines 53-56: network (i.e. flow) switch, identification information) Harkinson does not disclose encryption/decryption performed within the network interface and decryption completed prior to being routed by another flow switch. However, Williams discloses:

ii) a cryptographic module that decrypts, prior to, cipher text transaction requests and provides plain text transaction requests to the flow switch, wherein, prior to decryption, the cipher text transaction requests have not been routed by another flow switch. (see Williams col. 6, lines 56-57; col. 5, lines 39-43; col. 5, lines 19-24; col. 7, lines 17-23: encryption performed within network interfaces, before information processing by server)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson to enable encryption capabilities within network interfaces for connected network nodes as taught by Williams. One of ordinary skill in the art would be motivated to employ Williams in order to provide a high level of security assurance in a policy based security implementation within a network environment. (see Williams col. 4, lines 39-42: "*... provides a unique implementation of cryptographic technology with high-assurance policy-*

based enforcement of packet flow ... prevents unauthorized users from gaining access to sensitive information ... ")

Regarding Claim 39, Harkinson discloses the arrangement of claims 38, wherein, first and second encrypted transaction requests (see Harkinson col. 3, lines 5-7: simultaneous connections) are received from different clients having a common electronic address and served substantially simultaneously by different informational servers (see Harkinson col. 2, lines 46-54; col. 11, lines 46-49: common addresses for multiple members (i.e. information servers)), wherein at least some of the responses include a cookie and a tag identifying a previously selected informational server to service transaction requests from the client, wherein the cookie and tag are generated by the previously selected informational server, and wherein the flow switch uses the tag in the parsed plain text equivalent of each transaction request to select an appropriate informational server to service each of the first and second transaction requests. (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch ; col. 18, lines 40-43; col. 22, line 63 - col. 23, line 4: SSL (i.e. cookie, server generated) techniques utilized ; col. 11, lines 59-67: tag mode, message information utilized for server selection, two consecutive messages processed by same switch)

Regarding Claims 47, 62, Harkinson discloses the arrangement of claims 38, 53, further comprising: at least one traffic manager located between the content director and one or more clients to effect load balancing across a plurality of content directors. (see Harkinson col. 17, lines 41-43; col. 17, lines 48-50: distribute (i.e. balance) system

load across members, (i.e. server, content directors))

Regarding Claim 48, Harkinson discloses the arrangement of claim 38, wherein the content director includes a current connection table listing active connections between servers and clients, the current connection table comprising, for a selected invariant, a session identifier identifying a session with a client, a persistency timestamp indicating when a last transaction request was received from a client for the selected invariant, and cookie name and value. (see Harkinson col. 12, lines 44-47; col. 15, lines 3-9; col. 31, lines 37-38: active connections tracking ; col. 18, lines 40-43; col. 23, line 63 - col. 24, line 4: SSL (i.e. cookie) techniques utilized)

Regarding Claims 49, 64, Harkinson discloses the arrangement of claims 38, 53, wherein the flow switch is operable to tag a transaction response, the tag identifying an informational server generating the transaction response. (see Harkinson col. 11, lines 53-56; col. 11, lines 59-64: identifying information (i.e. tag) utilized to track information requests/responses ; col. 11, lines 59-67: tag mode, message information utilized for server selection)

Regarding Claims 50, 65, Harkinson discloses the arrangement of claims 49, 64, wherein at least sonic of the responses include a cookie, wherein the cookie is generated by the informational server previously assigned by the flow switch to service transaction requests from the client, and wherein the cookie is different from the tag.

(see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch interconnects servers ; col. 18, lines 40-43; col. 22, line 63 - col. 23, line 4: SSL (i.e. cookie) techniques utilized in information processing)

Regarding Claims 51, 66, Harkinson discloses the arrangement of claims 50, 65, wherein the tag is concatenated to the cookie. (see Harkinson col. 18, lines 40-43; col. 22, line 63 - col. 23, line 4: identification information mechanism, SSL (i.e. cookie) techniques utilized ; col. 11, lines 59-67: tag mode, message information utilized for server selection)

Regarding Claim 53 , Harkinson discloses in an arrangement comprising a plurality of informational servers connected to a communications network, all of the informational servers having a common address on the communications network and serving a set of information to clients, each of the informational servers being configured to receive a transaction request associated with an individual transaction and to provide a response to each transaction request, a method for serving transaction requests from clients, comprising:

b) the first flow switch parsing the plain text transaction request to locate one or more selected fields; (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch ; col. 11, lines 53-56; col. 11, lines 59-64: identification information utilized for information processing ; col. 2, lines 46-54: requests processed and passed to servers)

c) the first flow switch, based on the one or more selected fields, selecting an appropriate informational server to service the transaction request; (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch ; col. 11, lines 53-56; col. 11, lines 59-64: identification information utilized for information processing ; col. 2, lines 46-54: requests processed and passed to servers) and

d) the first flow switch thereafter forwarding at least portions of the plain text transaction request to a selected one of the informational servers, wherein the cipher text transaction request is decrypted prior to the parsing and selecting steps and wherein, prior to the decrypting step, the cipher text transaction request has not been directed to a flow switch other than the first flow switch. (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch ; col. 11, lines 53-56; col. 11, lines 59-64: identification information utilized for information processing ; col. 2, lines 46-54: requests processed and passed to servers)

Harkinson discloses parsing and informational server selection by the flow switch (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48; col. 11, lines 53-56: network (i.e. flow) switch, identification information) Harkinson does not disclose encryption/decryption performed within the network interface and decryption completed prior to being routed by another flow switch. However, Williams discloses:

a) a cryptographic module decrypting a cipher text transaction request to provide a plain text transaction request to a first flow switch; (see Williams col. 6, lines 56-

57; col. 5, lines 39-43; col. 5, lines 19-24; col. 7, lines 17-23: encryption performed within network interfaces, before information processing by server)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson to enable encryption capabilities within network interfaces for connected network nodes as taught by Williams. One of ordinary skill in the art would be motivated to employ Williams in order to provide a high level of security assurance in a policy based security implementation within a network environment. (see Williams col. 4, lines 39-42: "*... provides a unique implementation of cryptographic technology with high-assurance policy-based enforcement of packet flow ... prevents unauthorized users from gaining access to sensitive information ...* ")

Regarding Claim 54, Harkinson discloses the arrangement of claim 53, wherein, first and second encrypted transaction requests (see Harkinson col. 3, lines 5-7: simultaneous connections) are received from different clients having a common electronic address and served substantially simultaneously by different informational servers (see Harkinson col. 2, lines 46-54; col. 11, lines 46-49: common addresses for multiple members (i.e. information servers)), wherein at least some of the responses include a cookie and a tag identifying a previously selected informational server to service transaction requests from the client, wherein the cookie and tag are generated by the previously selected informational server, and wherein the flow switch uses the tag in the parsed plain text equivalent of each transaction request to select an appropriate informational server to service each of the first and second transaction

requests. (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch ; col. 18, lines 40-43; col. 22, line 63 - col. 23, line 4: SSL (i.e. cookie, server generated) techniques utilized ; col. 11, lines 59-67: tag mode, message information utilized for server selection, two consecutive messages processed by same switch)

Regarding Claim 61, Harkinson discloses the arrangement of claim 42, wherein the digest value is determined according to the following equation: L = h(K), where O<= L<=M, for all keys K, where K is at least a portion of the invariant, h is the hash function, L is the location of Kin the table, and M is the size of the table. (see col. 12, lines 1-5; col. 12, lines 10-13: data structure (i.e. hash table) generated for search (i.e. indexing) utilized a size parameter)

Regarding Claim 63, Harkinson discloses the arrangement of claim 53, wherein the content director includes a current connection table listing active connections between servers and clients, the current connection table comprising, for a selected invariant, a session identifier identifying a session with a client, a persistency timestamp indicating when a last transaction request was received from a client for the selected invariant, and cookie name and value, wherein, prior to decrypting step, the cipher text transaction request has not been directed to a flow switch other than the first flow switch. (see Harkinson col. 12, lines 44-47; col. 15, lines 3-9; col. 31, lines 37-38: active connections tracking ; col. 18, lines 40-43; col. 23, line 63 - col. 24, line 4: SSL (i.e. cookie) techniques utilized)

Regarding Claim 68, Harkinson discloses a computer readable medium comprising instructions to perform the steps of claim 53. (see Harkinson col. 30, line 64 - col. 31, lines 1; col. 31, lines 8-10: software (i.e. computer readable medium) to embody an information server processing system)

Regarding Claim 69, Harkinson discloses an arrangement for serving information requests, comprising:

a) a plurality of informational servers connected to a communications network, all of the informational servers having a common address on the communications network (see Harkinson col. 2, lines 26-28: multiple members (i.e. information servers)) and serving a set of information to clients, each of the informational servers being configured to receive a transaction request associated with an individual transaction and to provide a response to each transaction request; (see Harkinson col. 2, lines 46-54: client information requests, server responses) and

b) a content director (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch, (i.e. content director, information controller)) connecting the informational servers to the communications network and distributing transaction requests among the informational servers comprising:

i) a flow switch that parses plain text transaction requests to locate selected packet payload fields, selects, based on plain text packet payload fields, an

appropriate informational server to service each transaction request, and thereafter forwards at least portions of the parsed transaction requests to a selected one of the informational servers; (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch ; col. 11, lines 53-56; col. 11, lines 59-64: identification information utilized for information processing ; col. 2, lines 46-54: requests processed and passed to servers ; col. 11, lines 59-67: tag mode, message information utilized for server selection) and

Harkinson discloses parsing and informational server selection by the flow switch (see Harkinson col. 9, lines 15-23; col. 11, lines 53-56: network (i.e. flow) switch, identification information) Harkinson does not disclose encryption/decryption performed within the network interface and decryption completed prior to being routed by another flow switch. However, Williams discloses:

ii) a cryptographic module that decrypts, prior to, cipher text transaction requests and provides plain text transaction requests to the flow switch, wherein, prior to decryption, the cipher text transaction requests have not been routed by another flow switch. (see Williams col. 6, lines 56-57; col. 5, lines 39-43; col. 5, lines 19-24; col. 7, lines 17-23: encryption performed within network interfaces, before information processing by server)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson to enable encryption capabilities within network interfaces for connected network nodes as taught by Williams. One of

ordinary skill in the art would be motivated to employ Williams in order to provide a high level of security assurance in a policy based security implementation within a network environment. (see Williams col. 4, lines 39-42: "*... provides a unique implementation of cryptographic technology with high-assurance policy-based enforcement of packet flow ... prevents unauthorized users from gaining access to sensitive information ...* ")

Regarding Claim 70, Harkinson discloses the arrangement of claim 69, wherein, first and second encrypted transaction requests (see Harkinson col. 3, lines 5-7: simultaneous connections) are received from different clients having a common electronic address and served substantially simultaneously by different informational servers (see Harkinson col. 2, lines 46-54; col. 11, lines 46-49: common addresses for multiple members (i.e. information servers)), wherein at least some of the responses include a cookie and a tag identifying a previously selected informational server to service transaction requests from the client, wherein the cookie and tag are generated by the previously selected informational server, and wherein the flow switch uses the tag in the parsed plain text equivalent of each transaction request to select an appropriate informational server to service each of the first and second transaction requests. (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch ; col. 18, lines 40-43; col. 22, line 63 - col. 23, line 4: SSL (i.e. cookie, server generated) techniques utilized ; col. 11, lines 59-67: tag mode, message information utilized for server selection, two consecutive messages processed by same switch)

Regarding Claim 75, Harkinson discloses the arrangement of claim 69, wherein the first flow switch means is operable to tag a transaction response, the tag identifying an informational server generating the transaction response, wherein at least some of the responses include a cookie, wherein the cookie is generated by the informational server previously assigned by the first flow switching means to service transaction requests from the client, wherein the cookie is different from the tag, and wherein the tag is concatenated to the cookie. (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: network (i.e. flow) switch utilized to control information processing ; col. 11, lines 53-56; col. 11, lines 59-64: identification information (i.e. tag) utilized in information processing ; col. 18, lines 40-43; col. 22, line 63 - col. 23, line 4: SSL (i.e. cookie techniques) utilized)

Regarding Claim 76, Harkinson discloses the arrangement of claim 69, wherein the first flow switching means is capable to tag a transaction response, the tag identifying an informational server generating the transaction response, wherein at least some of the responses include a cookie, wherein the cookie is generate by the informational server previously assigned by the first flow switching means to service transaction requests from the client, wherein the cookie is different from the tag, and wherein the tag is concatenated to the cookie. (see Harkinson col. 9, lines 15-23; col. 9, lines 45-48: switch ; col. 18, lines 40-43; col. 22, line 63 - col. 23, line 4: cookie capabilities ; see Harkinson col. 11, lines 59-67: tag mode, packet payload (i.e. message information), message information utilized for server selection, two consecutive messages processed

by same switch)

6. **Claims 42, 43, 46, 57, 58, 72, 74** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hankinson-Williams** as applied to claims 38, 40; 53, 55; 69, 71 above, and further in view of **Schmeidler** (US 6,763,370) and **Kekic et al.** (US 6,763,370).

Regarding Claims 42, 57, 58, 72, Harkinson discloses wherein the content director generates a data structure based on request information, but Harkinson does not specifically disclose the generated hash (i.e. digest) value used as an index parameter for data structure. However, Schmeidler discloses the arrangement of claims 40, 42, 55, 71, wherein:

a) a digest generator that generates, when the hit counter for an invariant indicates at least a threshold transaction request receipt frequency, a digest value pointing to the location in the table where the corresponding entry is stored; (see Schmeidler col. 18, lines 44-51: hash (i.e. digest) generation techniques) and

b) a digest store that stores the digests corresponding to frequently requested content. (see Schmeidler col. 18, lines 44-51: hash (i.e. digest) generation techniques)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson to utilize encryption technology in the generation of a hash (i.e. digest) value to be used as an table index parameter as

taught by Schmeidler. One of ordinary skill in the art would be motivated to enhance Harkinson in order to strengthen security for data structures defining transaction information. (see Schmeidler col. 4, lines 34-47: *"... a server apparatus connectable over a computer network to one or more requestor processes ... "*; col. 29, lines 10-13: *"... virtual store front server 215 and database 213 are coupled to cache server 210 over a private, secure local area network 205 ..."*)

Regarding Claim 43, Harkinson discloses the generation of a data structure based on request information (see Harkinson col. 12, lines 1-5; col. 12, lines 10-13: data structure (i.e. hash table)), but Harkinson does not specifically disclose the generated hash value used as an index parameter for a data structure. However, Schmeidler discloses the arrangement of claim 42, wherein the digest store includes a digest value for each frequently requested invariant (see Schmeidler col. 18, lines 44-51: hash (i.e. digest) generation techniques)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson to use encryption techniques to generate a hash (digest) value used as an index as taught by Schmeidler. One of ordinary skill in the art would be motivated to enhance Harkinson in order to strengthen security for data structures defining transaction information. (see Schmeidler col. 4, lines 34-47; col. 29, lines 10-13)

Regarding Claims 46, 74, Harkinson discloses the arrangement of claims 42, 72,

wherein the digest value is determined according to the following equation: L = h(K), where O<= L<=M, for all keys K, where K is at least a portion of the invariant, h is the hash function, L is the location of Kin the table, and M is the size of the table. (see col. 12, lines 1-5; col. 12, lines 10-13: data structure (i.e. hash table) generated for search (i.e. indexing) utilized a size parameter)

7. **Claims 40, 41, 44, 45, 55, 56, 59, 60, 71, 73** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hankinson-Williams** as applied to claims 38, 53, 69, above, and further in view of **Kekic et al.** (US 6,763,370).

Regarding Claims 40, 55, 71, Harkinson discloses the arrangement of claims 38, 53, 69, wherein the content director further comprises:

b) a cache processor that accesses the plurality of objects in response to communications received from the flow switch. (see Harkinson col. 15, lines 49-54; col. 18, lines 21-23: cache (i.e. frequent usage) techniques utilized))

Harkinson discloses wherein a cache that stores a plurality of objects corresponding to transaction requests associated with the plurality of informational servers, the objects comprising a hot invariant table identifying information frequently requested from the informational servers, the hot invariant table including (see Harkinson col. 15, lines 49-54; col. 18, lines 21-23: cache (i.e. hot variant, hotness, frequent usage) techniques utilized), for each invariant identifying corresponding information. (see Harkinson col. 11, lines 53-56; col.

11, lines 59-64: identification information utilized in member (i.e. information server) processing) Hankinson does not specifically disclose updating a counter and performing a pre-determined action when a threshold is surpassed. However, Kekic discloses:

a) a hit counter indicating a number of transaction requests, received over a determined time interval, requesting the corresponding information; (see Kekic col. 27, lines 12-18: threshold processing utilizing a counter parameter)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson to utilize a counter for the occurrence of monitored events and the performance of a pre-determined action when a threshold is surpassed as taught by Kekic. One of ordinary skill in the art would be motivated to modify Harkinson in order to effectively monitor event occurrences. (see Kekic col. 4, line 66 - col. 5, line 4: *"... network management solution for computer networks having a computer network management capability ... efficiently manages a constantly changing and growing heterogeneous computer network ...")*

Regarding Claims 41, 56, Harkinson discloses the arrangement of claims 40, 55, wherein each invariant in the table further has a corresponding timestamp indicating when the respective entry was last updated, and a tag identifying a corresponding informational server providing the corresponding information. (see Harkinson col. 27, lines 21-26: time information utilized within communications processing)

Regarding Claims 44, 59, Harkinson discloses wherein the information corresponding to the invariant is served by a cache informational server and not an origin informational server. (see Harkinson col. 5, lines 55-58: specific functional members (i.e. servers)) Hankinson does not specifically disclose updating a counter and performing a pre-determined action when a threshold is surpassed. However, Kekic discloses the arrangement of claims 40, 55, wherein, when the hit counter for an invariant indicates at least a threshold transaction request receipt frequency. (see Kekic col. 27, lines 12-18: counter with a threshold)

> It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson to utilize a counter for the occurrence of monitored events and the performance of a pre-determined action when a threshold is surpassed as taught by Kekic. One of ordinary skill in the art would be motivated to modify Harkinson in order to effectively monitor event occurrences. (see Kekic col. 4, line 66 - col. 5, line 4)

Regarding Claims 45, 60, Harkinson discloses wherein the information corresponding to the invariant (see Harkinson col. 11, lines 53-56; col. 11, lines 59-64: identification information) is served by an origin informational server and not a cache informational server. (see Harkinson col. 5, lines 55-58: functional member (i.e. server)) Hankinson does not specifically disclose updating a counter and performing a pre-determined action when a threshold is surpassed. However, Kekic discloses the arrangement of claims 40, 59, wherein, when the hit counter for an invariant falls below a threshold

transaction request receipt frequency. (see Kekic col. 27, lines 12-18: counter with a threshold)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson to utilize a counter for the occurrence of monitored events and the performance of a pre-determined action when a threshold is surpassed as taught by Kekic. One of ordinary skill in the art would be motivated to modify Harkinson in order to effectively monitor event occurrences. (see Kekic col. 4, line 66 - col. 5, line 4)

Regarding Claim 73, Harkinson discloses wherein the invariant and information corresponding to the invariant is processed by a cache informational server and/or an origin informational server. (see Harkinson col. 11, lines 53-56; col. 11, lines 59-64: identification information processed by members (i.e. servers) ; col. 5, lines 55-58: functional members (i.e. servers)) Hankinson does not specifically disclose updating a counter and performing a pre-determined action when a threshold is surpassed. However, Kekic discloses the arrangement of claim 70, wherein, when the hit counter for an invariant indicates at least a threshold transaction request receipt frequency and the hit counter for an invariant falls below a threshold transaction request receipt frequency. (see Kekic col. 27, lines 12-18: counter processing utilizing a threshold parameter)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson to utilize a counter for the occurrence of monitored events and the performance of a pre-determined action when a threshold is

surpassed as taught by Kekic. One of ordinary skill in the art would be motivated to modify Harkinson in order to effectively monitor event occurrences. (see Kekic col. 4, line 66 - col. 5, line 4)

8. **Claims 52, 67** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Harkinson-Williams** as applied to claims 38, 49; 53, 64; above, and further in view of **Sato et al.** (US Patent No. 6,748,446) and **Burkett et al.** (US Patent No. 6,671,853).

Regarding Claims 52, 67, Harkinson discloses the arrangement of claims 50, 64, wherein, during a first time interval, the flow switch is in a tagging mode in which the switch generates and appends tags to transaction responses and, during a second different time interval, the switch operates in a digesting mode in which digests are generated, invariant hotness is monitored, and transaction requests are routed to informational servers based on requested invariant hotness and/or cookie and wherein, during the first time interval, the flow switch does not operate in the digesting mode and, during the second time interval the flow switch does not operate in the tagging mode. (see Harkinson col. 11, lines 53-56; col. 11, lines 59-64: identification information utilized in member (i.e. information server) processing ; col. 15, lines 49-54; col. 18, lines 21-23: cache (i.e. hotness, frequent usage) techniques utilized ; Harkinson col. 11, lines 59-67: tag mode, packet payload (i.e. message information), message information utilized for server selection, two consecutive messages processed by same switch)

Harkinson discloses wherein the capability for a messaging system to operate in tag mode. (see Harkinson col. 11, lines 59-67: tag mode, packet payload (i.e. message information), message information utilized for server selection, two consecutive messages processed by same switch)

Sato discloses wherein the capability to operate a messaging system in a digest mode. (see Sato col. 3, lines 39-46; col. 6, lines 1-7: client/server ; col. 6, lines 54-59; col. 6, lines 54-59; col. 12, lines 22-29: digest mode (i.e. message grouping) capabilities for messaging) And, Burkett discloses the capability to transition a messaging system between two operational modes (i.e. tag and digest). (see Burkett col. 7, lines 15-18: client/server ; col. 4, lines 39-46: transition between two operational modes (i.e. tag mode and binary mode), analogous art)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harkinson for a messaging system to operate in digest mode as taught by Sato, and to enable transition of operating modes as taught by Burkett. One of ordinary skill in the art would be motivated to employ Sato in order to enable the efficient delivery of information services and good quality media data (see Sato col. 1, lines 59-65: *" ... provides merits such as quick response of information services and good quality of delivered data ... client to obtain data at the information source upstream from the delivery server ... from a site nearer to the client having a good access environment, i.e., good audio and video data quality ... "*), and to employ Burkett in order to enable the capability for the efficient storage of static and changeable information (see Burkett col. 3, line 64 - col. 4, line 2: *" ... include both static information*

and changeable information ... store static portions of the information in serialized, binary format while storing changeable information with its tags in a tagged document format would enable the advantages ... to be realized ... ").

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
February 4, 2006

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100